IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

G.T., by and through next friend LILIANA T. HANLON, SHIMERA JONES, LEROY JACOBS, BALARIE COSBY-STEELE, JOHN DEMATTEO, RICHARD MADAY, MARK HEIL, ALLISON THURMAN, and SHERIE HARRIS, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

SAMSUNG ELECTRONICS AMERICA, INC. and SAMSUNG ELECTRONICS CO., LTD.,

Defendants.

Civil Action No: 1:21-cv-04976

Hon. Nancy L. Maldonado

SAMSUNG ELECTRONICS AMERICA, INC.'S AND SAMSUNG ELECTRONICS CO., LTD.'S MOTION AND MEMORANDUM IN SUPPORT OF MOTION <u>TO DISMISS THE CONSOLIDATED AMENDED CLASS ACTION COMPLAINT</u>

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Defendants Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. (collectively, "Samsung") move under Federal Rule of Civil Procedure 12(b)(6) to dismiss Plaintiffs' Consolidated Amended Class Action Complaint ("CAC") for the reasons stated below.

I. <u>INTRODUCTION</u>

Plaintiffs' claims should be dismissed because their factual allegations demonstrate that the statute upon which their claims are based—the Illinois Biometric Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA")—plainly does not apply to Samsung's photo-viewing Gallery App. The Illinois legislature passed BIPA to address the risk of identity theft that might occur when an individual's "biometrics" are compromised. 740 ILCS 14/5(c). Biometrics are unique physical characteristics of a specific individual. 740 ILCS 14/5(c); *see also* CAC ¶ 34. BIPA regulates two categories of biometrics: "biometric identifiers" and "biometric information." 740 ILCS 14/10. "Biometric identifiers" exclude photographs and physical descriptions, and "biometric information" similarly "does not include information derived from" those photographs and descriptions. *Id.* An entity that "collect[s]" or "otherwise obtain[s]" biometrics must provide written notice and obtain prior authorization. 740 ILCS 14/15(b). Once "in possession of" biometrics, private entities must develop and publish data retention and destruction policies. 740 ILCS 14/15(a).

Plaintiffs contend that Samsung violated BIPA through a function of the Gallery App, which is pre-installed on Samsung smartphones and tablets. CAC ¶¶ 2, 3, 50. They allege that the Gallery App "organize[s] and sort[s] photos based upon the particular individuals who appear in the photos." *Id.* ¶ 55. They further allege that to accomplish this sorting, the Gallery App uses an algorithm that scans a user's photographs for faces, "create[s] a unique digital representation known as a 'face template,'" and compares templates using "'face clustering,' which analyzes each image for facial 'landmarks,' extracts those key facial features when found, and converts said data into 'vectors,' each of which is assigned a numerical value corresponding to a specific facial feature." *Id.* ¶¶ 4, 53, 55. In this motion, Samsung refers to the alleged face templates and data produced in the face clustering analysis collectively as "Face Clustering Data." Plaintiffs allege that Face Clustering Data is stored in a database "that is kept at least on the solid state memory on the user's Samsung Device." *Id.* ¶ 54. Even accepting Plaintiffs' factual allegations about the Gallery App' operation as true for purposes of this motion, both of their counts must be dismissed.

First, Plaintiffs' BIPA claims fail because Plaintiffs have not made—and cannot make—the requisite factual allegations to show that Samsung is "in possession of," "collect[s]," "capture[s]," or "otherwise obtain[s]" the Face Clustering Data. 740 ILCS 14/15(a), (b). Plaintiffs correctly concede that the Face Clustering Data is stored locally in the solid state memory on Plaintiffs' devices. *See, e.g.,* CAC ¶¶ 5, 54, 57, 58, 60, 64, 73-74. They do not allege that the Face Clustering Data is stored anywhere ***beyond*** Plaintiffs' own devices. Indeed, Plaintiffs do not allege any facts to establish that any mechanism exists for Samsung to obtain or access the Face Clustering Data, let alone that Samsung actually retrieved, obtained, or had access to it. (Nor would they be able to cure that failure, given that Samsung provided them with a sworn declaration to the contrary.) Instead, Plaintiffs conflate Samsung's control over the design of the software app with control of the Face Clustering Data that is generated when users (like Plaintiffs) use that software. *See id.* ¶¶ 60-65. But as courts have repeatedly recognized in a variety of contexts, simply selling a device does not give the device manufacturer "possession" or "control" over user-generated data. Were it otherwise, Microsoft would be deemed to have possession of and control over this motion by virtue of counsel using Microsoft Word to draft it. As detailed in Section III(A), numerous courts have declined to hold a product manufacturer and seller liable where it does not collect or otherwise obtain the data that is alleged to be a biometric identifier or biometric information. Plaintiffs' failure to allege any facts that plausibly show Samsung obtains or even has access to any Face Clustering Data is dispositive and requires dismissal of all of their BIPA claims.

Second, Plaintiffs cannot state a BIPA claim because the Face Clustering Data is not a "biometric identifier" or "biometric information" regulated under BIPA. BIPA is intended to cover "biometrics," which are unlike "other unique identifiers" because they are "biologically ***unique to [an] individual***." 740 ILCS 14/5(c) (emphasis added). This language focusing on the nature of biometrics as a unique identifier shows that the statute applies to data that can be used to ***identify*** an individual. Plaintiffs do not allege that the Face Clustering Data identifies who the individuals are—they concede that Plaintiffs themselves made that identification. *E.g.,* CAC ¶ 180. Plaintiffs allege that facial recognition technology generally (not specifically the Gallery App) can be used to compare biometric identifiers to a database and "[i]f a database match is found, an individual may be identified." *Id.* ¶ 38. But with respect to the Gallery App, Plaintiffs do not allege that the software compares biometric identifiers to a database to confirm an individual's identity. They allege that the Gallery App compares the Face Clustering Data generated from newly stored photos to the Face Clustering Data of individuals in previously stored photos, *id.* ¶¶ 55-56, 88-90, 101-104, and that if a match is found, the Gallery App "tags" the newly stored photo and "groups it with previously stored images depicting the same individual." *Id.* ¶ 56. Thus, they allege that the Gallery App can sort photos based on the software's determination that those photos are likely to contain images of the same person, not that it can ascertain who that person is. The Gallery App does not and cannot identify to whom the faces belong. One Plaintiff acknowledges that it was he—***not*** Samsung—who identified the individuals in his photos when he "tagged" them. *Id.* ¶ 180. Plaintiffs do not allege that they needed the Face Clustering Data to know the identities of the people in those photos or that Plaintiffs used the data to learn them.

Plaintiffs' CAC should be dismissed in its entirety and with prejudice.

II. LEGAL STANDARD

Dismissal is warranted when a complaint fails to allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); Fed. R. Civ. P. 12(b)(6). Claims are facially plausible only "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Garrard v. Rust-Oleum Corp.*, 575 F. Supp. 3d 995, 999 (N.D. Ill. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citations omitted)). Under the *Twombly/Iqbal* standard, the Court "need not accept as true statements of law or unsupported conclusory factual allegations." *Yeftich v. Navistar*, 722 F.3d 911, 915 (7th Cir. 2013). Instead, the Court may "draw on its judicial experience and common sense" to determine "whether a complaint states a plausible claim for relief." *Iqbal*, 556 U.S. at 679.

III. ARGUMENT

A. Plaintiffs' BIPA Claims Fail Because Samsung Does Not "Possess," "Collect," "Capture," or "Otherwise Obtain" Face Clustering Data.

Plaintiffs do not and cannot state a claim that Samsung violated either Section 15(a) or Section 15(b) of BIPA because they do not plausibly allege that Samsung collected or is in possession of the Face Clustering Data. To state a claim under BIPA Section 15(a), Plaintiffs must allege facts showing that Samsung was "in possession" of biometric data. 740 ILCS 14/15(a). BIPA does not specifically define "possession," so Illinois federal and state courts have applied the term's "popularly understood meaning" as its "settled legal meaning"—that is, "possession" occurs when the defendant held the data at its disposal or exercised dominion or control over the data, which in turn depends on whether the defendant "could freely access the data" and "how [the defendant] allegedly received it." *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. Feb. 24, 2020) (citing *People v. Ward*, 215 Ill. 2d 317, 325 (2005) as the basis for its definition of "possession"); *see also Jacobs v. Hanwha Techwin Am., Inc.,* 2021 WL 3172967, at *3 (N.D. Ill. Jul. 27, 2021) (using the same language and citing *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 284 (N.D. Ill. 2019)); *Barnett v. Apple Inc.*, 2022 IL App (1st) 220187 at ¶¶ 41-42 (Ill. App. Ct. 1st Dist. Dec. 23, 2022) (also citing *Ward*, 215 Ill. 2d at 325); *Mora v. J&M Plating, Inc.*, 2022 IL App (2d) 210692, at ¶ 38 n.5 (Ill. App. Ct. 2d Dist. Nov. 30, 2022) (same; reversing summary judgment on other grounds).

Similarly, to state a claim under Section 15(b), Plaintiffs must allege facts showing that Samsung collected, captured, or otherwise obtained biometric data. 740 ILCS 14/15(b). Illinois courts have construed the term "capture" as used in BIPA to mean "to record in a permanent file" and the term "collect" to mean that information is "gathered or accumulated from a number of persons into one place." *Barnett*, 2022 IL App (1st) 220187 at ¶¶ 49-50 (citing *Mosby v. Ingalls Memorial Hospital*, 2022 IL App (1st) 200822 (Ill. App. Ct. 1st Dist. Sept. 30, 2022)). And courts have construed the term "otherwise obtain" to mean to bring information into one's own possession, especially through effort. *See, e.g., Heard*, 440 F. Supp. 3d at 966. Courts have further held that Section 15(b) only applies where any acquisition of the data involves an "active step" by the defendant. *Heard*, 440 F. Supp. 3d at 966; *Jacobs,* 2021 WL 3172967, at *2-3.

Plaintiffs' own allegations show that they cannot satisfy the required elements of their BIPA claims. While Plaintiffs make only a conclusory allegation that Samsung "systematically captures, collects, uses, and stores the highly-sensitive Biometrics," CAC ¶ 57, they have not alleged any facts to make those allegations plausible. Rather, the facts that they do plead show that Samsung does *not* collect, capture, or obtain Face Clustering Data. Plaintiffs allege that the Gallery App is pre-installed on a user's phone, *id.* ¶¶ 3, 50; that the Gallery App runs on a user's device and generates Face Clustering Data, *id.* ¶¶ 52-57; and that the user-generated Face

Clustering Data is stored locally on that user's device, as opposed to a centralized location, *id.* ¶¶ 5, 54, 76. Plaintiffs do ***not*** allege that Samsung itself obtained or assembled into one place user-generated Face Clustering Data, that Samsung ever accessed that data stored locally on users' phones, or that Samsung even has the ability to access that data stored locally on users' phones. The failure and inability to plead those facts is fatal to Plaintiffs' BIPA claims. *See Barnett*, 2022 IL App (1st) 220187 at ¶ 46 (affirming dismissal where plaintiffs alleged information was stored on users' individual devices, not defendant's databases).

Plaintiffs' new assertion that Face Clustering Data is stored "at least" locally on users' devices, *id.* ¶¶ 5, 54, does not cure their pleading deficiencies. Plaintiffs have done nothing more than substitute the words "at least" into the allegation from the First Amended Complaint ("FAC") that Face Clustering Data is stored ***only*** on users' devices. *See* FAC ¶ 25. Plaintiffs still have not alleged any facts or identified a location other than the user's device where Face Clustering Data is stored. Nor could they. Instead, Plaintiffs allege that ***photographs*** can be stored to a cloud server. CAC ¶¶ 51, 66. But Plaintiffs do not allege that Face Clustering Data is or can be similarly stored. Plaintiffs cannot mask these deficiencies by removing their prior concession that Samsung "does not store or transfer" Face Clustering Data on or by means of its servers. FAC ¶ 34. Alleging that Face Clustering Data ***Plaintiffs*** generate locally on their devices is stored "at least" on ***Plaintiffs'*** devices, CAC ¶ 5, 54, without alleging any facts that Samsung can access the data from the users' devices or any other place means the allegations are still not sufficient to state a BIPA claim, which requires that a defendant actually collect, capture, obtain, or possess the data.

In the CAC, Plaintiffs allege that Samsung has control over, and therefore possesses, the Face Clustering Data because Samsung designed the Gallery App, pre-installed it on their phones, and controls what data the Gallery App collects. *See* CAC ¶¶ 50, 60-65. But Plaintiffs' conclusory allegations of Samsung's control over design decisions about pre-installed software on Plaintiffs' phones do not mean that Samsung "possessed" data that is later generated and stored locally on Plaintiffs' devices while the devices are in Plaintiffs' possession. *Contra id.* ¶ 60 (confusing control over software design with control over data on individual phone). Their strained construction of the word "possession" is flatly inconsistent with the statutory text and the precedent interpreting it. *See Heard*, 440 F. Supp. 3d at 968; *Jacobs*, 2021 WL 3172967, *3 (holding that "possession occurs when someone exercises any form of control over the data or held the data at his disposal") (internal marks omitted); *Barnett*, 2022 IL App (1st) 220187 at ¶¶ 43-44; *Ward,* 215 Ill. 2d at 325.

Other courts considering allegations similar to those made here have held that such allegations fail to plead possession. The *Barnett* court affirmed dismissal of claims that Apple had violated BIPA by providing software that allowed users to extract their fingerprints or face geometries to unlock their devices and authorize purchases. 2022 IL App (1st) 220187. The *Barnett* plaintiffs argued that Apple "possessed" their face geometries and fingerprints because "Apple software" on the device "collects and analyzes their information." *Id.* at ¶ 43. The court rejected this argument and affirmed dismissal of the complaint, holding that plaintiffs' argument wrongly "equates the product with the company." *Id.* The court explained, "[t]he device and the software are the tools, but it is the user herself who utilizes those tools to capture her own biometric information" and there was no allegation that Apple collected or stored that information on a separate server. *Id.* at ¶ 44.[1] Other decisions have similarly confirmed that a device manufacturer

[1] While *Barnett* also noted that the plaintiffs in that case, not Apple, could decide whether to use the feature, that was an independent reason to distinguish *Hazlitt*. 2022 IL App (1st) 220187 ¶ 46 ("*Hazlitt* is distinguishable because the plaintiffs in *Hazlitt* alleged that Apple stored the facial information in Apple's own database ***and*** that users had no power to delete the collected information or disable the feature on their devices.") (emphasis added). Moreover, the *Barnett* court factually distinguished another case on the sole ground that "[t]he Complaint in this case does not allege that Plaintiffs' biometric information was sent to Apple's servers or any third party server." *Id.* (distinguishing *Zaluda v. Apple*, No. 2019-CH-11771 (Cir. Ct. Cook County, Oct. 29, 2020)).

is not in possession of data the user generates merely by virtue of having designed the technology. *E.g.*, *Heard*, 440 F.Supp.3d at 964, 968-969 (rejecting BIPA claim against fingerprint scanner manufacturer where manufacturer did not own, operate, or have access to the data allegedly obtained through the scanners); *Jacobs,* 2021 WL 3172967, at *3-4 (dismissing claims that a camera manufacturer "possessed" or "controlled" data from its cameras where a department store that purchased and had the cameras installed—***not*** the manufacturer—owned, operated, and had access to the data allegedly obtained through the cameras). *Accord Stauffer v. Innovative Heights Fairview Heights, LLC*, No. 19-L-311 at 3 (St. Clair Cnty., Ill., July 23, 2022) (dismissing Section 15(a) claim where defendant never took "actual direct possession of the data"). Here, Plaintiffs' own factual allegations show that Samsung is in the same position as the defendants in *Barnett, Heard*, *Jacobs*, and *Stauffer*: while Samsung may have supplied the device that had functionality used by the Plaintiffs, it does not receive or have the ability to access the data that the user generates, so there is no collection, capture, or possession of that data.

Cases where BIPA claims have survived motions to dismiss confirm that Plaintiffs' allegations here are fatally deficient. In *Hazlitt v. Apple*, for example, the court allowed BIPA claims to survive a motion to dismiss based on the court's understanding that plaintiffs had alleged that Apple could access the data at issue. *See* 500 F. Supp. 3d 738, 751-52 (S.D. Ill. 2020) (*"Hazlitt I*") ("[I]f what Plaintiffs allege is true, [Apple] collects the biometric data into a facial recognition database on the device that ***Apple alone can access.***") (emphasis added) (distinguishing *Heard* and other cases on that basis); *id.* at 751 (noting outcome could be different if allegation – not found in the CAC here – was not correct); *Hazlitt v. Apple, Inc*., 543 F. Supp. 3d 643, 653 (S.D. Ill. 2021) ("*Hazlitt II*") ("Plaintiffs also claim . . . that Apple alone could access the biometric data"). The court in *Hazlitt* thus confirmed that the manufacturer's ongoing access would be a necessary predicate for any BIPA claim. That key point is underscored in later proceedings in *Hazlitt*, where an amended complaint alleged expressly that "Apple automatically transfers [the] Sync Data . . . [at issue] to Apple's servers via the cloud" and that "Apple maintains and stores encryption keys that enable it to access the Sync Data." *Hazlitt v. Apple*, No. 3:20-CV-421-NJR, Dkt. 135 at 11 (S.D. Ill. Aug. 1, 2022) (ruling on subsequent motion to dismiss) ("*Hazlitt III*").

In *Barnett*, the court found that *Hazlitt* was factually distinguishable in part "because the plaintiffs in *Hazlitt* alleged that Apple stored the facial information in Apple's own databases" whereas in *Barnett* "it is alleged that the information is stored, not on Apple's databases, but on the user's individual devices and that users may delete the information and disable the features." *Barnett*, 2022 IL App (1st) 220187 at ¶ 46; *see also id.* (noting that to the extent plaintiff advocates a broader reading of *Hazlitt*, it is unpersuasive and based on an untested interim decision). Here too, Plaintiffs' inability to factually allege data transmission to, storage by, or access by Samsung invalidates their BIPA claims. In contrast to the plaintiffs in the *Hazlitt* proceedings, Plaintiffs here make no factual allegation that Samsung has any encryption keys or ability to access that data that resides on their phones. They cannot hide this pleading deficiency by removing the concession from the FAC that Samsung "does not store or transfer" Face Clustering Data on or by means of its servers, *compare to* FAC ¶ 34, particularly where the CAC still does not assert any factual allegations contrary to the prior concession.

Similarly, the reasoning in *Namuwonge* supports Samsung. In that case, an employee alleged that a workforce timekeeping device manufacturer was liable under BIPA, even though the devices were owned and operated by his employer, not the manufacturer. 418 F. Supp. 3d at 283, 285. The court dismissed the Section 15(b) claim because the employee had failed to allege facts showing that the manufacturer actively collected biometric data. *Id.* at 286. And while the court allowed the Section 15(a) claim to survive, it did so because the employee alleged that the employer "disclosed . . . employees' fingerprint data to [the manufacturer]," which the court reasoned was sufficient to establish "possession" under BIPA. *Id.* at 284. No such disclosure to Samsung is alleged here.

Adopting Plaintiffs' view that Samsung should be deemed to "possess" information it never received and could not access also would be inconsistent with Section 15(a)'s destruction requirement. 740 ILCS 14/15(a). If Plaintiffs were correct, to comply with Section 15(a) Samsung would have to build new capabilities to (a) continually monitor customers' use of its devices to determine the last date of use of the Gallery App, and then for a further three years, and (b) access the device and permanently destroy the data stored in it by the user. Effectively requiring manufacturers to engage in biometric collection so it could then destroy that data would be at odds with BIPA's purpose. *See Stauffer,* No. 19-L-311 at 3 (dismissing Section 15(a) claim where defendant never took "actual direct possession of the data," and thus "[could not] destroy it").

Numerous courts have rejected contentions that a technology manufacturer should be deemed to possess or to have collected, captured, or otherwise obtained, user-generated biometric data by virtue of having developed and distributed technology that can be used by others to generate such data. *E.g.*, *Barnett*, 2022 Il App (1st) 220187 (affirming dismissal); *Heard*, 440 F. Supp. 3d at 966 (dismissing BIPA claim); *Jacobs*, 2021 WL 3172967, at *3 (same). Indeed, several more cases decided since *Hazlitt I* and *II* confirm that the inquiry under Sections 15(a) and (b) turns on whether the plaintiff adequately alleged that the defendant ***itself*** accessed, collected, or possessed the alleged biometrics. *Compare Barnett*, 2022 Il App (1st) 220187 (no Section 15(a) and 15(b) claims where plaintiffs only alleged data was stored on their personal devices); *Stauffer v. Innovative Heights Fairview Heights, LLC*, 2022 WL 3139507, at *4 (S.D. Ill. Aug. 5, 2022) (dismissing Section 15(b) claim where plaintiff did not allege that defendant stored, used, or accessed biometric information); *with Karling v. Samsara Inc.*, 2022 WL 2663513, at *6 (N.D. Ill. July 11, 2022) (plaintiff adequately stated Section 15(b) claim where it alleged that defendant "stored [plaintiff's] biometric information in its cloud-based dashboard, and then provided access to that dashboard and services based on that data to his employer").

Because Samsung does not possess, collect, capture, or otherwise obtain Plaintiffs' biometric information or Biometric identifiers, Plaintiffs cannot state a BIPA claim for the additional reason that they have not been aggrieved by any violation of statute. BIPA provides that "[a]ny person aggrieved by a violation of this Act shall have a right of action … against an offending party." *See* 740 ILCS 14/20 (emphasis added). Regardless of whether there has been a violation of the Act (and there has not), Plaintiffs' biometric data is expressly alleged to reside on devices that are in their possession, and there is no allegation that any third party has access to that data. Accordingly, Plaintiffs cannot assert any claim under BIPA.

B. Plaintiffs Have Failed to Plead a BIPA Claim Because The Face Clustering Data Does Not Identify Particular Individuals.

Plaintiffs have no claim under BIPA for the independent reason that BIPA does not regulate the Face Clustering Data. BIPA regulates "biometric identifiers" and "biometric information," the "biologically unique" data identifying specific individuals. 740 ILCS 14/5 (discussing legislative findings and intent of BIPA). BIPA defines the term "biometric identifier" to mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and "biometric information" to mean information "used to identify an individual" that is "based on an individual's biometric identifier." 740 ILCS 14/10. For example, an individual's thumbprint is "biometric identifier," and an electronically-stored version of that thumbprint associating that thumbprint with a particular individual is "biometric information." *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d

1197, 1203 (Ill. 2019) ("Six Flags"). Plaintiffs do ***not*** allege, nor could they, that the Face Clustering Data identifies particular individuals. Rather Gallery App users (including Plaintiffs)—if they choose—may use the tagging feature within the Gallery App to associate identifying information (or any other label of their choosing) with Face Clustering Data. And Plaintiffs do ***not*** allege, nor could they, that if they mis-identified an individual through the tagging feature, the Gallery App has the ability to correct that error.

BIPA's language repeatedly reinforces that the Illinois legislature intended BIPA to protect data identifying specific individuals. The section of that statute setting forth the "legislative findings and intent" explains: "Biometrics are unlike other unique identifiers" and they "are biologically unique to the individual." 740 ILCS 14/5(c). The statute's focus is thus on data that uniquely identifies an individual, and BIPA's statutory language must be interpreted in light of that statutory purpose. *See generally Lacey v. Vill. Of Palatine*, 904 N.E.2d 18, 25 (Ill. 2009) (holding that a court must give effect to the legislature's intent as evidenced by the plain language of a statute). The remainder of the statute reinforces this legislative purpose. It imposes obligations with respect to "biometric ***identifiers***," a phrase that inherently by its name involves identification of an individual, and "biometric information," which is defined as "information based on an individual's biometric identifier ***used to identify an individual.***" 740 ILCS 14/10 (emphasis added). Section 15(a) requires private entities in possession of biometric data to destroy that data "when the initial purpose for collecting [it] . . . has been satisfied or within 3 years of ***the individual's*** last interaction with the private entity." 740 ILCS 14/15(a) (emphasis added). And Section 15(b) prohibits collecting, capturing, purchasing, receiving through trade, or otherwise obtaining "***a person's*** or ***a customer's*** biometric identifier or biometric information." 740 ILCS 14/15(b) (emphasis added). Accordingly, if the data cannot be used to identify a specific individual, it does not qualify as a "biometric identifier" or "biometric information."

Plaintiffs fail to allege facts that the Face Clustering Data the Gallery App generates either identifies or can be used to identify particular individuals. Plaintiffs do allege that one ***potential*** use of facial recognition technology is to match a "face template" to an identified individual. CAC ¶ 38. But they make no such allegations about Samsung's Gallery App. Rather, Plaintiffs allege that the Gallery App can organize and sort photos by comparing the Face Clustering Data of individuals in newly stored photos against Face Clustering Data of individuals in already-stored photos to determine if a match exists. *Id.* ¶ 55-56, 88-90, 101-104. Plaintiffs then allege that if a match is found, Samsung "assigns a tag based on the objects, faces, or individuals identified, and saves it to the Gallery App." *Id.* ¶ 52. But this "tag" is not a person's identity. Plaintiffs do ***not*** allege, nor could they, that the Gallery App itself (or Samsung) supplies any information in these tags that provides the identity of any specific, named individual in the photos. The actual identification of an individual can only be made by the user of the device. *E.g., id.* ¶ 180 ("Plaintiff Maday . . . has 'tagged' individuals in photographs that Samsung has organized by facial geometry.") Plaintiffs do not allege the Face Clustering Data can identify who the individuals in the photos are. To the contrary: users' own knowledge, not the technology, is what may identify people in their photographs, if users elect to create a tag with accurate identifying information to associate with the Face Clustering Data for any given individual appearing in their photographs.

The CAC thus is distinguishable from complaints that have survived dismissal motions by alleging the defendant maintained a centralized database that was used to determine the actual identity of individuals appearing in photographs (as opposed to determining only that the photos likely include images of the same unidentified person). *Cf. e.g.*, *In re Facebook Biometric Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016); *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103

(N.D. Ill. 2015); *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017); *Hazlitt I*, 500 F. Supp. 3d 738; *Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017). The complaints against Facebook, Shutterfly, and Google alleged that those defendants leveraged databases of face templates that the defendants maintained so that defendants could suggest to users the identity of the *specific* individuals appearing in their users' photographs. For example:

(i) The *Facebook* complaint expressly alleged that Facebook stored users' facial recognition data in its ***own*** databases. *See* Complaint, *In re Facebook*, No. 3:15-cv-03747-JD, Dkt. 40 ¶¶, 43, (N.D. Cal. Aug. 28, 2015) ("Facebook subsequently stored Licata's biometric identifiers in its databases."); *id.* ¶ 50 ("Facebook subsequently stored Patel's biometric identifiers in its databases.").

(ii) Similarly, the *Shutterfly* complaints alleged that Shutterfly's "tag suggestion" feature "works by comparing the face templates of individuals who appear in newly-uploaded photos with the facial templates already ***saved in Defendants' face database*** . . ." . Complaint, *Norberg v. Shutterfly*, No. 1:15-cv-05351, Dkt. 6 ¶ 22 (N.D. Ill. Jun. 23, 2015) (emphasis added); Complaint, *Monroy v. Shutterfly, Inc*, No. 16-cv-10984, Dkt. 1 ¶ 23 (N.D. Ill. Nov. 30, 2016) (substantially same).

(iii) The *Google* complaint alleged that the facial recognition technology for the cloud-based Google Photos "works by comparing the face templates of individuals who appear in newly-uploaded photos with the facial templates already saved in ***Google's face database***." Complaint, *Rivera v. Google, Inc.*, No. 1:16-cv-02714, Dkt. 40 ¶¶ 22-23 (N.D. Ill. May 27, 2016) (emphasis added).

(iv) Similarly, in *Hazlitt,* the plaintiff had alleged that Apple's photos app "collects the biometric data into a facial recognition database on the device that Apple alone can access." 500 F. Supp. 3d at 751.

Here, Plaintiffs pointedly did not allege—and indeed could not allege—that Samsung maintains a database of Face Clustering Data that identifies particular individuals. If the user wishes to identify any Face Clustering Data with an individual, that is the user's choice, and that information is neither generated by nor available to Samsung. Plaintiffs' carefully-wordsmithed pleading pointedly does not allege that Samsung maintains such a database, and instead refers to a "database" that is alleged to exist *only* on the user's own device and to which Samsung is not alleged to have access. *See* CAC ¶ 5 ("Each face template is stored in a facial recognition database on, at least, the user's Samsung Device in the solid state memory …"); *id.* ¶ 76 (alleging information stored on multiple user devices, not a centralized Samsung database). Accordingly, because the Face Clustering Data generated by Samsung's Gallery App does not identify particular individuals, it is not a "biometric identifier" or "biometric information" governed by BIPA. That alone warrants dismissal of Plaintiffs' claims.

IV. **CONCLUSION**

Plaintiffs have failed to plead allegations that (if true) would show that Samsung engaged in any conduct prohibited under BIPA. Accordingly, the Court should dismiss Plaintiffs' Consolidated Amended Class Action Complaint with prejudice.

Dated: January 30, 2023

By: /s/ Mark H. Boyle
Mark H. Boyle

ATTORNEY FOR DEFENDANTS
SAMSUNG ELECTRONICS AMERICA, INC. and
SAMSUNG ELECTRONICS CO., LTD.

DONOHUE BROWN MATHEWSON & SMYTH LLC
Mark H. Boyle
131 South Dearborn Street, Suite 1600
Chicago, IL 60603
(312) 422-0900

O'MELVENY & MYERS LLP
Randall W. Edwards
Matthew D. Powers (*pro hac vice*)
Two Embarcadero Center, 28th Floor
San Francisco, CA 94111-3823
(415) 984-8700

O'MELVENY & MYERS LLP
Ashley M. Pavel
610 Newport Center Dr., 17th Floor
Newport Beach, CA 92660
(949) 823-6900

Attorneys for Samsung Electronics America, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the 30th of January, 2023, he caused the foregoing DEFENDANT SAMSUNG ELECTRONICS AMERICA, INC.'S MOTION TO DISMISS THE AMENDED CLASS ACTION COMPLAINT to be filed with the Clerk of the District Court via the CM/ECF system, which will send notification of such filing to all counsel of record at the email addresses on file with the Court.

By: /s/ Mark H. Boyle
Mark H. Boyle

ATTORNEY FOR DEFENDANT
SAMSUNG ELECTRONICS AMERICA, INC.

DONOHUE BROWN MATHEWSON &
SMYTH LLC
Mark H. Boyle
131 South Dearborn Street, Suite 1600
Chicago, IL 60603
(312) 422-0900